(12) INTERNATIONAL APPLICATION PUBLISHED UNDER THE PATENT COOPERATION TREATY (PCT)

CORRECTED VERSION

(19) World Intellectual Property Organization
International Bureau

(43) International Publication Date
28 April 2005 (28.04.2005)

PCT

(10) International Publication Number
WO 2005/038818 A1

(51) International Patent Classification[7]: H04L 9/08

(21) International Application Number:
PCT/SE2004/001466

(22) International Filing Date: 13 October 2004 (13.10.2004)

(25) Filing Language: English

(26) Publication Language: English

(30) Priority Data:
60/510,153 14 October 2003 (14.10.2003) US

(71) Applicants and
(72) Inventors: **SELANDER, Göran** [SE/SE]; Bergsundsgatan 25, S-117 37 Stockholm (SE). **LINDHOLM, Fredrik** [SE/SE]; Stamgatan 87, S-125 74 Älvsjö (SE). **NYSTRÖM, Magnus** [SE/SE]; Hälsingevägen 15, S-186 35 Vallentuna (SE).

(74) Agent: **AROS PATENT AB**; P.O. Box 1544, S-751 45 Uppsala (SE).

(81) Designated States *(unless otherwise indicated, for every kind of national protection available)*: AE, AG, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BW, BY, BZ, CA, CH, CN, CO, CR, CU, CZ, DE, DK, DM, DZ, EC, EE, EG, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MA, MD, MG, MK, MN, MW, MX, MZ, NA, NI, NO, NZ, OM, PG, PH, PL, PT, RO, RU, SC, SD, SE, SG, SK, SL, SY, TJ, TM, TN, TR, TT, TZ, UA, UG, US, UZ, VC, VN, YU, ZA, ZM, ZW.

(84) Designated States *(unless otherwise indicated, for every kind of regional protection available)*: ARIPO (BW, GH, GM, KE, LS, MW, MZ, NA, SD, SL, SZ, TZ, UG, ZM, ZW), Eurasian (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM), European (AT, BE, BG, CH, CY, CZ, DE, DK, EE, ES, FI, FR, GB, GR, HU, IE, IT, LU, MC, NL, PL, PT, RO, SE, SI, SK, TR), OAPI (BF, BJ, CF, CG, CI, CM, GA, GN, GQ, GW, ML, MR, NE, SN, TD, TG).

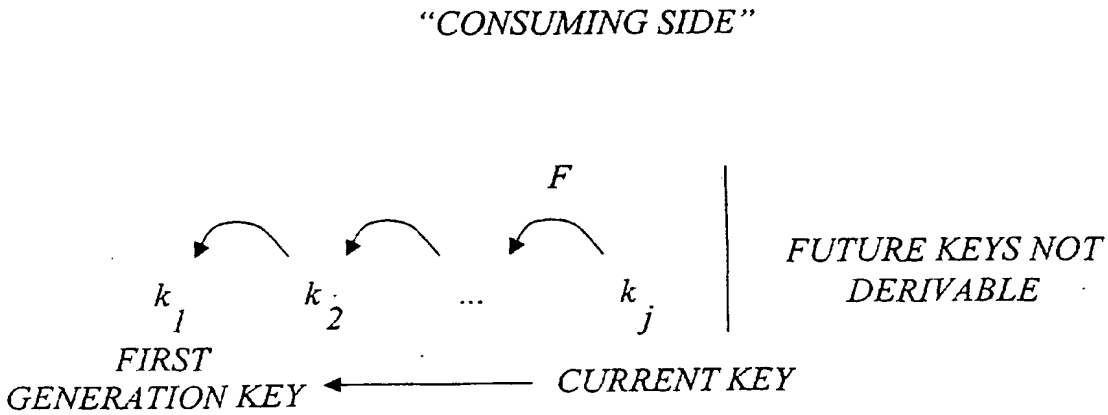
Published:
— *with international search report*
— *before the expiration of the time limit for amending the claims and to be republished in the event of receipt of amendments*

(48) Date of publication of this corrected version:
9 June 2005

(15) Information about Correction:
see PCT Gazette No. 23/2005 of 9 June 2005, Section II

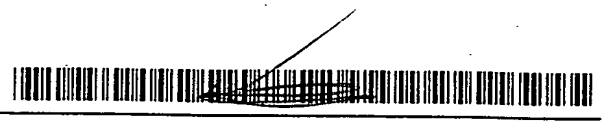
[Continued on next page]

(54) Title: EFFICIENT MANAGEMENT OF CRYPTOGRAPHIC KEY GENERATIONS



(57) Abstract: The invention generally relates to management of cryptographic key generations in an information environment comprising a key-producing side generating and distributing key information to a key-consuming side. A basic concept of the invention is to define, by means of a predetermined one-way key derivation function, a relationship between generations of keys such that earlier generations of keys efficiently may be derived from later ones but not the other way around. A basic idea according to the invention is therefore to replace, at key update, key information of an older key generation by the key information of the new key generation on the key-consuming side. Whenever necessary, the key-consuming side iteratively applies the predetermined one-way key derivation function to derive key information of at least one older key generation from the key information of the new key generation. In this way, storage requirements on the key-consuming side can be significantly reduced.

WO 2005/038818 A1



For two-letter codes and other abbreviations, refer to the "Guidance Notes on Codes and Abbreviations" appearing at the beginning of each regular issue of the PCT Gazette.